The Use of AI in monitoring SIEM Tools

January 10th 2021

Researched by A.Etesami

Introduction

Security Information and Event Management (SIEM) tools provide organisations with the ability to centralise the collation and analysis of data from multiple sources to identify and mitigate potential threats.

If implemented and configured correctly, SIEM tools can alert the monitoring team to failed logins, malware, and other potentially malicious activities.

Large organisations will produce petabytes of data that can overwhelm their people and systems causing suspicious events to be missed.

The question that this paper aims to address is whether the use of Artificial Intelligence (AI) can improve the performance of the Security Operating Centres (SOC) and their SIEM tools. In order to answer this question, this paper also explores the following questions:

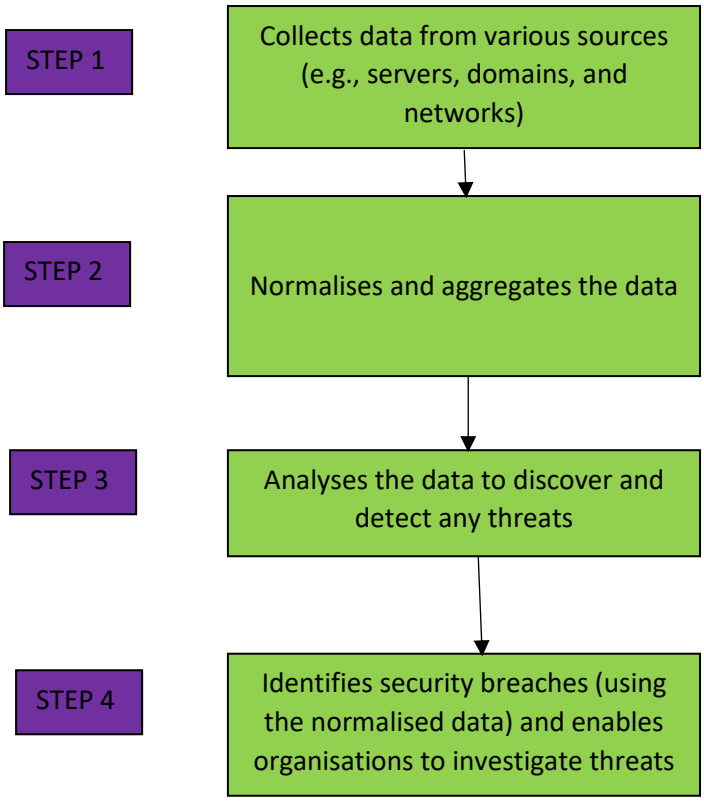
- How can AI be used in SIEM?
- Why is AI in SIEM important to the security of data?
- How is AI linked to automation?
- What are the advantages of AI in SIEM?
- What are the disadvantages of AI in SIEM?

What is SIEM?

SIEM tools are an important part of the data protection ecosystem: they aggregate data from different systems and analyse data to capture suspicious activity or possible cyber-attacks. SIEM tools provide a central location for capturing events and warnings, but they can be costly, resource intensive, and customers complain that issues with SIEM data are often difficult to fix.

In addition, the analysts who are required to configure and operate the SIEM tools are scarce and expensive resources who need extensive training in order to become effective.

The following graph shows the step-by-step process of SIEM tool.



SIEM tools function by gathering logs, reviewing log data for risks, and monitoring performance. Today's SIEM solutions have a range of specialised features to ensure information security, with some of the most notable features being:

- Logging – SIEM tools collect log data from system components, the data is then normalised and centralised within SIEM. This ensures that the data can then be used to gather insights into current and past security events,
- Threat Analysis – Uses the data from logging, compares it with the database and identifies any particular patterns which might be associated with a security threat,
- Response – Once a threat has been identified, SIEM sends out data implicating that there has been an attack on the security. Quicker detection leads to quicker response, therefore eliminating any issues before they cause damage. With automaton, SIEM tools can also automate a solution with tool-driven actions.

An attack signature is a special information arrangement that can be used to mark the effort of an attacker to exploit a known flaw to the operating system or program. When an attack signature is observed by Intrusion Detection, it displays a Security Warning.

The problem is that sophisticated attackers are constantly inventing or reinventing more effective ways to mount their assaults. Traditional legacy security designed to keep out attackers or spot these attacks occurring can miss these ever-changing threat behaviours allowing the attacker to breach the security of the system.

- **The Evolution of SIEM**

The definition of security information and event management (SIEM) has its roots in the need for a coherent view of security incidents across various technologies. From antivirus software detecting malware at any endpoint to a firewall on an Internet connection, SIEM provides security operation teams with a single dashboard from which to determine the security model of their organisations.

Over the years, standards have risen from these systems, with manufacturers arguing that their SIEM platforms can also be used to link isolated incidents and detect risks that individual protection products would otherwise miss. Given the growing importance of cyber security, this technology has quickly risen to the top of many organisations' arsenal of tools who want to improve and update their security.

- **Incident Responses**

SIEM provides different capabilities in response to incidents that occur:

- Reporting security incidents using the threat detection software built within SIEM,
- Alerts organisations based on analytics and patterns for any threats, indicating security breach.

IT Departments requires a coordinated way to handle and manage possible infringements. The effects of incident responses are to minimize harm and reduce recovery time and costs. Therefore, incident responses are important in getting data and information to the organisation quickly, so that they can act accordingly and prevent any sort of attacks, whilst maintaining their security model.

- **Benefits and Drawbacks of SIEM Tools**

SIEM applications provide a powerful method of threat identification, real-time monitoring and long-term security log and event analysis. This method can be extremely useful for the safety of enterprises of all sizes.

Benefits of SIEM include:

- Increased efficiency,
- Preventing potential security threats,
- Reducing costs,
- IT compliance,
- Efficient reporting of threats,
- Reducing the impact of security breaches.

Drawbacks of SIEM include:

- SIEM is only as useful as the data that is put into it,
- If the SIEM does not have a feed from a particular asset that is under attack then it cannot detect that attack,
- More data does not mean better detection, due to some data being irrelevant, or data is repeated,
- High maintenance, especially when AI is implemented into SIEM,
- The tuning of SIEM systems is critical to get a balance between reducing the number of alerts that being raised to a level that can be investigated by the Security Operations Centre and not filtering out events that which would give an indication that an attack is under way.

- **Advanced Threat Intelligence**

  Security threats are constantly changing due to the new methods and procedures criminals use to obtain information of a sensitive nature. Analytical SIEM tools will respond to new advanced threats through introducing network security monitoring, endpoint detection and behaviour analysis in conjunction with each other to recognize and isolate new potential threats. Most firewalls and intrusion detection systems do not have these features on their own, therefore SIEM tools are used to fill in for these missing features.

  The aim of threat intelligence is to not only detect threats, but also to assess the nature of these threats by determining the origin after it has been initially identified, how that threat should be contained, and how information should be exchanged.

What is Artificial Intelligence

Artificial Intelligence (AI) is a technology that enables a machine to 'think' or behave in a way that deduces the correct response to a situation by applying rules on what should done and working out how to apply those rules to the current situation. It does this by taking information from its surroundings and determining its answer based on what it observes or senses. Such technology already influences the way we live, work, and have fun in our spare time, even without us realising it. AI is becoming a greater part of our lives, as the technology behind it is becoming more and more advanced. Machines are developing their ability to 'learn' from mistakes and improve the way they perform a job the next time perform it.

AI can be used for many different tasks and activities. Personal electronic devices or accounts (such as our phones or social media) use AI to learn more about us and the things we do digitally. One example of this is streaming services like Netflix that use AI technology to understand what we like to watch and suggest other shows to us based on the

information Netflix gathers for every second we are on the application and comparing our pattern of watching to other peoples in order to find shows that we might like to watch.

- **Narrow, General and Super AI**
  The definition of AI is not widely agreed. However, there is a distinction between 'General AI' and 'Narrow AI'. All current AI can be defined as Narrow AI. It is generally agreed that General AI is a long time away. However, the strongest form of AI out of the three is 'Super AI', where its capabilities will exceed human abilities.

  Artificial narrow intelligence (ANI), also referred to as narrow AI, is the only form of artificial intelligence that has been successfully realized to date. Narrow AI is goal-oriented, designed to perform unique tasks e.g., facial recognition, speech recognition/voice assistants, driving a car or searching the internet and is extremely capable in achieving the task it is programmed to perform.

  Artificial General Intelligence (AGI), also referred to as general AI, is the idea of a computer with general intelligence that mimics human intelligence and/or actions, with the ability to learn and use its intelligence to solve any problems. In any given situation, AGI will think, understand, and behave in a way that is indistinguishable from that of a human being.

  Artificial Super-Intelligence (ASI) is a hypothetical AI that not only mimics or recognizes human intelligence and behaviour but goes beyond it; ASI is when computers become self-conscious and exceed human intelligence and capacity. This sort of AI that is often seen as dangerous. For example, Elon Musk has stated that it would be too difficult to control the development of ASI if the hypothesis is true for ASI being more capable of human ability. (See https://www.independent.co.uk/life-style/gadgets-and-tech/news/elon-musk-artificial-intelligence-ai-singularity-a9640196.html)

- **Types of Machine Learning**
  - In **supervised learning**, the agent observes an example of input-output devices and learns the function that maps from input to output. For example, for object classification, training data could include several images of various fruit types and labels specifying which fruit is shown in each photo. The trained model is considered to generalise the fruits category if it can correctly recognize the fruit type when presented.
  - In **unsupervised learning**, the agent learns patterns in input even if no clear output is provided. For example, for image recognition, training data could include thousands of individual photographs of five types of animals, but no labels identifying the animals. The model is considered to work well if it is capable of correctly dividing the images into five piles, each containing pictures of one type of animal.
  - **Reinforcement learning** is a goal-oriented type of learning in which the agent develops over time based on being presented by positive and negative

outputs. For example, for recommendation systems, human listeners can recommend music based on their previous listening habits. The user gives feedback as to whether they like the auto-recommended track and this feedback helps the algorithm to learn the user's listening habits, which ensures that the recommendations become more reliable over time.

- **Adversarial AI**

Adversarial AI is the malicious creation and use of sophisticated digital technologies and systems that have intellectual mechanisms usually associated with human behaviour. These involve the ability to learn from previous experience and to uncover meaning from complicated data.

From this diagram, adversarial AI is used to manipulate an existing entity, in this case a photo of the Planet Jupiter, and transforms the meaning of that entity to something different, in this case an apple. Although to the naked eye we can still see Jupiter in both the existing image and the sum image, computers will understand the sum as an apple. The confidence percentage shows the percentage of certainty of the computer in identifying what the entity is. In this example, the computer has 64.5% certainty that the existing entity is Jupiter, therefore 35.5% uncertainty which can lead to misidentification. When looking at the sum image (Apple), the computer has 99.3% certainty that the image in an apple, which is a drastic increase from the existing certainty. This is deemed dangerous as Adversarial AI can manipulate any entity, using adversarial noise, to manipulate meanings out of entities, with having little to no uncertainty. We can use our imagination to see how dangerous this method can be, and the countless entities that could be choreographed into meaning something completely different.

- **Why AI is implemented into SIEM tools**

Developers have several reasons to integrate AI and SIEM. Simplifying and optimising the detection and analysis of different types of threats is one of the most important. Security software has evolved over time to improve the process for the detection and suppression of digital threats. However, it has not managed to get away from the classic antivirus (AV) software. AV software detect threats by using only information already in their databases. This makes them unable to detect unknown anomalies (known as zero-day attacks) because they do not have the

ability to identify new information to their own systems. This is a major problem in an era where cyber-attacks are getting more and more sophisticated every day.

Moreover, the rise in the volume of data treated by SIEM specialists on a regular basis continues to slow down the system. It is therefore almost impossible to continue to analyse large volumes of data manually or through traditional security software. This is where it is useful to integrate AI, so that it becomes more convenient and efficient in tackling cyber-attacks.

The potential for AI is that it can be used to identify the normal pattern of working for each individual account holder or each component of a system and then spot when events occur which are out of the ordinary and require further investigation.

For example, AI might be used to detect that an employee normally works between 9:00am to 5:30pm but over the last 2 weeks that employee has logged on during the middle of the night, possibly from a different workstation to one that they normally use and started using multiple applications that they do not normally use.

AI can weight each of these behaviours to see if a combination of changes in behaviour gives greater concern about the activities that are taking place, and so needs to be alerted as requiring an investigation.

AI and SIEM solutions can improve the performance of IT defence departments by identifying bugs, risks, and cyber-attacks. With limited human analyst interference, this technology has improved to detect unknown threat attacks. The integration of AI and SIEM enables IT protection teams to decrease the number of false / irrelevant details that need human intervention. In this way, to concentrate on higher priority tasks, SIEM analysts will transition their effort to validating relevant details.

- **How it works**

  Through using complex algorithms, computer security firms teach AI programs to detect viruses and malware so that AI can then do pattern detection in applications. This helps data protection providers to keep updated on the current threats and time frames to develop sensitive plans to protect enterprises.

  In cyber-security, AI and ML are of great importance. AI is great at distinguishing normal and anomalous behaviours in SIEM. Computer systems may be designed to prepare themselves by applying Machine Learning to increase their ability to identify unfamiliar safety factors and abnormalities. In cybersecurity, the use of these methods significantly increases the precision of threat identification. In addition, ML models will carry out investigations into identified threats and reduce the number of irrelevant details that exist in protecting systems.

In a business context, AI and ML-equipped security information and event management (SIEM) tools can easily structure the workflows for threat identification in the network.

- **Advantages and Disadvantages of AI in SIEM**

The advantages of using AI in SIEM tools are:

- AI's inherent ability to be scaled – therefore is efficient,
- Refined capabilities – Much more capable than human abilities at examining vast amounts of data and correlating data from multiple different sources,
- Reduce human involvement which reduces the risk or human error and the cost of people required to carry out the analysis,
- AI can simplify the identification, processing, and response to security threats,
- AI takes a calculated approach – therefore produces more consistent results,
- AI can simultaneously undertake multiple tasks – monitoring and protecting vast number of devices and systems, which means that it spot patterns of behaviour across multiple systems which would not be obvious to a human analyst and as a result can potentially identify 'zero day' attacks,
- Can mitigate large scale or sophisticated attacks.

The disadvantages of using AI in SIEM tools are:

- AI does not utilise valuable analyst skills directly and therefore does not benefit from human reasoning in possible explanations for unusual behaviours,
- Concerns relating to AI leading to organisations wishing remove the much needed human expertise in conducting the follow-up investigations,
- AI can be unpredictable – impossible to predict the evolution of AI,
- AI is difficult to maintain,
- AI could fall into the hands of wrong people – resulting in greater cyber security threats.

Companies taking advantage of AI in SIEM

Several large companies, including Microsoft and IBM, have developed advanced threat analytics to detect risks and react as malicious attackers change their tactics, leveraging algorithms relevant to user and object behaviour detection and machine learning.

As the knowledge base for its AI solution 'Watson for Defence', IBM has loaded its X-Force security research library as the knowledge base (See https://www.zdnet.com/article/how-australias-department-of-defence-is-using-ibm-watson/). In order to enhance its threat-detection accuracy and time, this security system can benefit from the library of security threats and feedback from security analysts.

Vectra uses AI through user experience analysis, vulnerability ratings, and internal and external threat detection, to detect ransomware threats.

Conclusion

As cyber-attacks become more frequent and sophisticated, it is important that organisations consider the available cyber defence resources available to them. There is a conflict between the amount of data and practicality of analysing this data when it comes to security monitoring. Although organisations do not want to skip a single security incident, it is simply difficult to handle all the notifications in security infrastructures from all the devices in enterprise infrastructure.

This is where SIEM can offer benefits. Through centralising all the alerts on a single platform, SIEM will inform of any incident that needs the expertise's attention. This allows the enterprise to maintain their security system and prevent any threats.

To automate the SIEM process, AI is implemented to 'amp up' security, and improve threat detection. AI can be used as a passive tool to identify threats and use SIEM's built in response and report capabilities to inform of any security breaches.

Using AI in SIEM can be very useful, but has some disadvantages, however overall, the benefits outweigh the drawbacks. AI in SIEM is already widely used around many enterprises and has great potential in improving security systems as it develops.